REVA
UNIVERSITY
Bengaluru, India

Detect,
Manage & Mitigate
CYBER RISKS

PGD / M.Tech. in
CYBERSECURITY
Powered by **AforeCybersec**

in Association with **IBM**

www.race.reva.edu.in

AforeCybersec
Securing The World Ahead

IBM

**IBM Software Lab for
Emerging Technologies**
Initiative of the Career Education Program

REVA
UNIVERSITY
Bengaluru, India

**In collaboration with
REVA University,** Bengaluru

DEMAND FOR CYBERSECURITY PROFESSIONALS OUTPACES SUPPLY

According to NASSCOM estimates, India needs one million cybersecurity professionals by 2020. Cybersecurity Ventures reports that there will be 3.5 million unfilled cybersecurity jobs by 2021, up from 1 million openings last year. The 2017 ISACA survey found that 45 percent of organizations out of 2,290 members in 121 countries reported they are hiring more cybersecurity professionals, but 94 percent stay it will prove difficult to find skilled candidates. The impetus of this program is to cater to this worldwide rise in demands for highly skilled cybersecurity professionals.

WHY STUDY CYBERSECURITY?

- Rise in global demand for skilled professionals.
- Cyber experts are needed in every industry & Sector.
- Most highly waged among IT professionals
- A profession with room for rapid career growth.
- Interesting, challenging and extremely dynamic work.
- A job with higher purpose and honour.

PROGRAM BENEFITS

- Learn from real-life scenarios using **Cyber Range & Security Operations Centre (SOC).**
- Industry certifications from **IBM.**
- Industry Leaders a faculty.
- Labs equipped with latest tools and technologies.
- 24/7 online support with resources, communities and interactions.
- Networking opportunities with industry leaders and professionals
- Weekend contact classes - designed for working professionals.
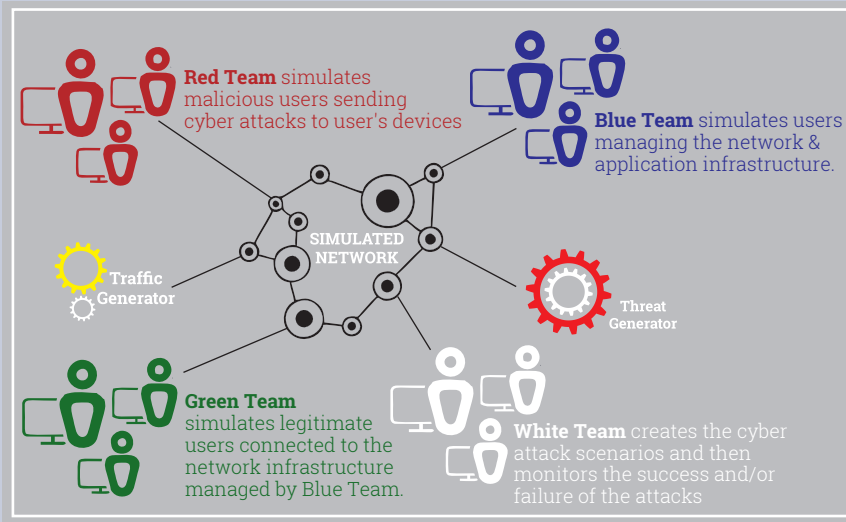- Lateral placement assistance.

CAREER OPTIONS IN CYBER SECURITY

- SECURITY ANALYST
- PENETRATION TESTER
- SOC SPECIALIST
- SOC ANALYST
- SIEM SPECIALIST
- SECURITY CONSULTANT

CYBER RANGE

Powered by AforeCybersec, Cyber Range systems, an infrastructure for Cyber Defence, simulates scenarios that prepare participants to manage the cybersecurity environment of corporate, military and government organizations. Cyber Range exercise is composed of multiple teams and each team is placed in a compartmentalized space that will reproduce a realistic enterprise network environment.

Red Team simulates malicious users sending cyber attacks to user's devices

Blue Team simulates users managing the network & application infrastructure.

SIMULATED NETWORK

Traffic Generator

Threat Generator

Green Team simulates legitimate users connected to the network infrastructure managed by Blue Team.

White Team creates the cyber attack scenarios and then monitors the success and/or failure of the attacks
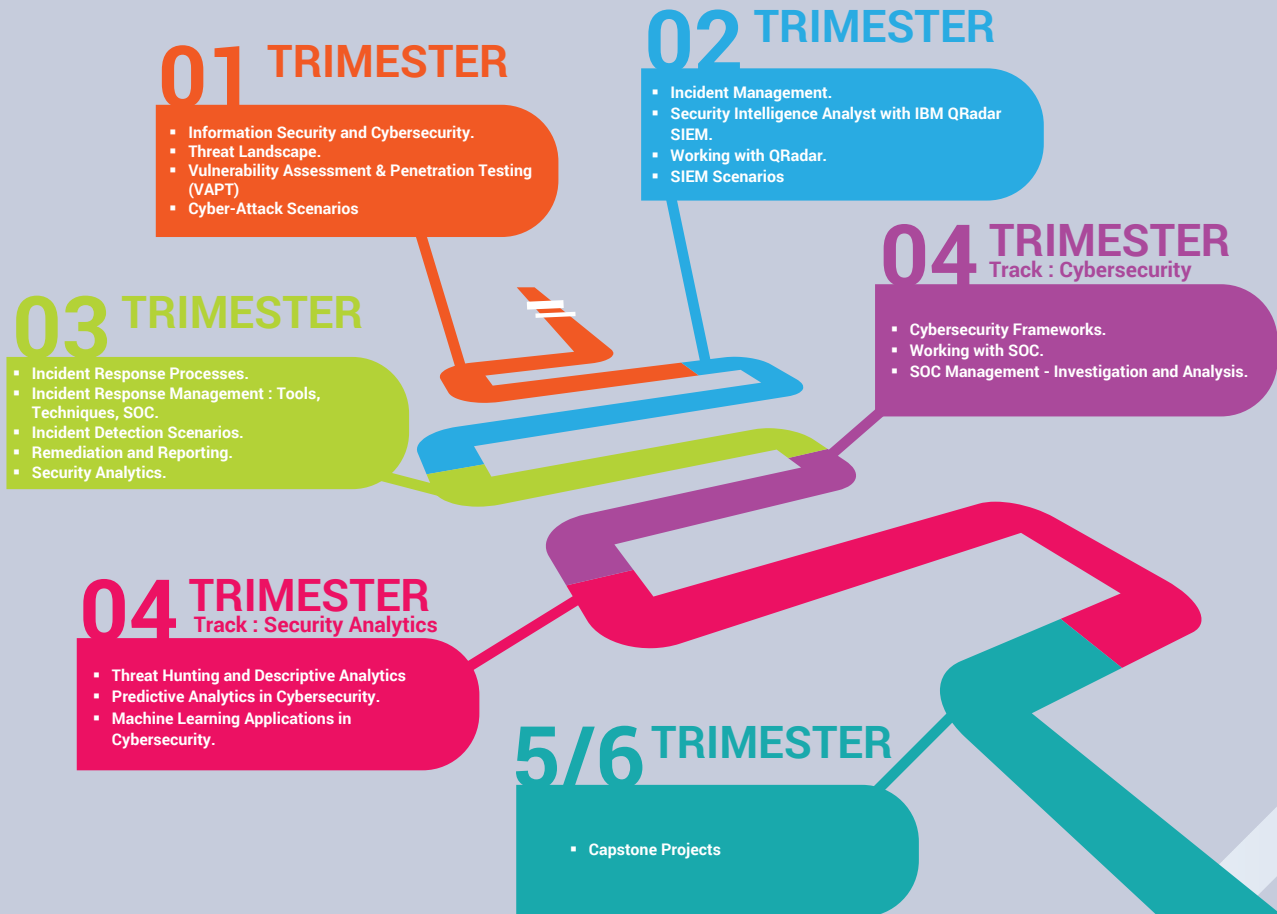
CYBER-ATTACK SCENARIOS

- Data Leakage
- Malicious Websites
- Botnet Communications
- Newly Emerging and Known Malwares

SECURITY OPERATIONS CENTER (SOC)

Participants will get access to Security Operations Centre (SOC), a live facility where the real-world simulation of an organization's enterprise information systems, including websites, data centre, servers, applications and other network platforms are monitored, assessed and protected from potential cyber threats.

Identity & Access Management

SIEM Log Monitoring

Network Security

Endpoint Security

Vulnerability Assessment & Penetration Testing

Threat & Vulnerability Management

Threat Intelligence

Compliance Analysis & Reporting

Incident Response

PROGRAM STRUCTURE

01 TRIMESTER
- Information Security and Cybersecurity.
- Threat Landscape.
- Vulnerability Assessment & Penetration Testing (VAPT)
- Cyber-Attack Scenarios

02 TRIMESTER
- Incident Management.
- Security Intelligence Analyst with IBM QRadar SIEM.
- Working with QRadar.
- SIEM Scenarios

03 TRIMESTER
- Incident Response Processes.
- Incident Response Management : Tools, Techniques, SOC.
- Incident Detection Scenarios.
- Remediation and Reporting.
- Security Analytics.

04 TRIMESTER
Track : Cybersecurity
- Cybersecurity Frameworks.
- Working with SOC.
- SOC Management - Investigation and Analysis.

04 TRIMESTER
Track : Security Analytics
- Threat Hunting and Descriptive Analytics
- Predictive Analytics in Cybersecurity.
- Machine Learning Applications in Cybersecurity.

5/6 TRIMESTER
- Capstone Projects

PGD in Cybersecurity (One Year) | M.Tech in Cybersecurity (Two Years)

WHO CAN APPLY?
- Two plus years of work experience in IT.
- 55 percent marks in BE/BTech/BCA/ME/MTech/MCA.
- Selection of the candidates are based on personal interviews.

CONTACTS

ADMISSIONS

Nivedha Yuvaraj
Phone: +91 9738368436
E-Mail: nivedhayuvaraj@reva.edu.in

Abhijit Sinha
Phone: +91 9538874441
E-Mail: abhijitsinha@reva.edu.in

PROGRAM OFFICE

Shinu Abhi, Ph.D. | Fulbright Fellow
Director- Corporate Training
(REVA Academy for Corporate Excellence-RACE)
Phone:+91 9972917030
E-Mail: race@reva.edu.in | shinuabhi@reva.edu.in

---

www.race.reva.edu.in

REVA University
Rukmini Knowledge Park, Yelahanka, Kattigenahalli, Bengaluru, Karnataka 560064